UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/874,292	06/06/2001	Gary Manuel Jackson	63795-0007	6320

24633 7590 12/31/2007

HOGAN & HARTSON LLP
IP GROUP, COLUMBIA SQUARE
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

NOTIFICATION DATE	DELIVERY MODE
12/31/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

dcptopatent@hhlaw.com

Office Action Summary	Application No.	Applicant(s)	
	09/874,292	JACKSON, GARY MANUEL	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,6-12,16-29 and 31-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3,4, 6-12, 16-29, 31-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3-4, 6-12, 16-29, 31-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Copeland III(2002/0144156) in view of Botros(6,769,066).

3. As per claims 1, 31, Copeland III discloses a method for detecting unauthorized intrusion in a network system(0016, 0033), receiving packet level activity information from the network(0019); collecting continuous sequential samples of port specific information from the received packet level activity information for each IP/user wherein many packets are accumulated in any one sampling interval for each IP/user(0018, 0037, 0060-0061, 0165), converting packet level activity into activities for each IP/user(0139, 0157); recognizing predefined and specific human behavior elements associated with normal and malicious activity for the accumulated activity from the accumulated packets in a sample of packet level activity(0157-0158, 0197). Copeland et al. does not disclose behaviors and activities for each IP/user with a designation of 1 equals present or 0 equals absent; and processing in real-time the presence or absence of identified behavior elements for each IP/user occurring within a set sampling interval with a pre-trained neural network behavior assessment pattern classifier into a behavior assessment measures the amount of expertise and deception present for each IP/user for a given sampling interval as measures of underlying malicious and non-malicious intent, the

trained pattern classifier converting any combination of the predefined behavior elements present for an IP/user for an IP/user for any sampling interval to non signature and non-anomaly identifying presence of at least one activity, assigning a binary representation 1 to indicate present, zero to indicate absent to the at least one identified activity, generating an assessment based upon the binary rating.

4. Botros discloses disclose behaviors and activities for each IP/user with a designation of 1 equals present or 0 equals absent(see col. 3, lines 34-37, col. 10, lines 42-48); and processing in real-time the presence or absence of identified behavior elements for each IP/user occurring within a set sampling interval with a pre-trained neural network behavior assessment pattern classifier into a behavior assessment measures the amount of expertise and deception present for each IP/user for a given sampling interval as measures of underlying malicious and non-malicious intent(see col. 3, lines 63-67, col. 4, lines 1-5, col. 10, lines 40-48), the trained pattern classifier converting any combination of the predefined behavior elements present for an IP/user for an IP/user for any sampling interval to non signature and non-anomaly based pattern classifier determined, assessments of the level of expertise and deception represented by the behavior elements present for that IP/User's sampling interval, and wherein if operator determined thresholds for degree of expertise and deception are exceeded, a network connection blocking action is activated automatically(see col. 6, lines 53-65, col. 8, lines 46-67, col. 13, lines 24-31).

5. It would have been obvious to one of ordinary skill in the art at the time of the invention to include indicating a presence or absence of behaviors for each IP/user of Botros with Copeland III, the motivation is that most attempted security violations are internal; that is, they

are attempted by employees of an enterprise or organization(see col. 1, lines 48-52). Botros discloses detecting computer network intrusions is calculated based upon factors such as command sequences, user activity, machine usage loads, resource violations, files accessed, data transferred, terminal activity and network activity. These factors or input to a model or expert system which determines whether a possible violation has occurred(see col. 1, lines 53-63). Thus, this is a method detects misuse of users within a network. It would have been obvious to one of ordinary skill in the art at the time of the invention to include identifying presence of at least one activity and assigning a binary representation to the activity of Botros et al. with Lyle, the motivation is that by identifying and assessing a binary rating using a histogram of Botros shows the feature values of all users over a predetermined period of time(see col. 11, lines 35-38).

6. Same motivation as above. As per claim 3, Botros et al. discloses wherein the step of generating an assessment includes associating the binary rating with an assessment based upon predetermined criteria(see col. 7, lines 1-67, col. 8, lines 1-40).

7. As per claims 4, 21, Botros et al. discloses wherein the step of generating an assessment includes mapping the assessment on at least one two-dimensional grid(see col. 11, lines 52-66, col. 12, lines 8-25). The motivation is that a histogram graph shows the distribution of a feature values for a selected feature for all users over a predetermined period of time(see Botros, col. 11, lines 36-38).

8. As per claim 6, Botros et al. discloses wherein the step of generating an assessment includes generating a profile of the IP/user based upon the monitored behavioral measures(see col. 7, lines 1-67, col. 8, lines 1-40). The motivation is that by generating an assessment based

upon behavioral measures, one can determine whether a user's activities or normal or deviates from past behavior(see col. 9, lines 1-3).

9. As per claim 7, Botros et al. discloses wherein the step of generating an assessment is carried out utilizing a back propagation network(see col. 12, lines 45-46). The motivation is that by including the back propagation network of Botros with Copeland, is that the back propagation network includes a training algorithm that is used in network intrusion detection, to distinguish between normal behavior and anomalous behavior (see col. 12, lines 25-51 of Botros).

10. Same motivation as above(see claim 7). As per claims 8, 16, Botros et al. discloses wherein the back propagation network includes psychological assessment information (see col. 12, lines 25-51).

11. Same motivation as claim 1. As per claim 9, Botros et al. discloses wherein the assessment is one of high deception and expertise and low deception and expertise (see col. 6, lines 53-65, col. 8, lines 46-67). The motivation is that by giving an assessment of high or low, anomalous or normal behavior can be scored accordingly (see col. 13, lines 24-41 of Botros).

12. Same motivation as claim 1. As per claims 10, 23-24, wherein the blocking action includes sending a blocking command to a firewall for blocking further network access, Botros inherently discloses this because Botros discloses a firewall(see col. 6, lines 31-45), if high deception and or high expertise exceeds threshold(see col. 6, lines 53-65, col. 8, lines 46-67, col. 13, lines 24-41).

13. As per claims 11, 25, Copeland III et al. discloses wherein the tracking action includes storing activity information in a tracking module(see 0055).

14. As per claim 26, Copeland III discloses wherein the tracking module includes a tracking database for storing activity information that may be used to provide evidence of an intruder's harmful intent activities and at least one intent assessment during a session(see 0055, 0066).

15. As per claim 27, Copeland III discloses wherein the tracking database includes neural network assessment and associated information for the intruder that is at least one of tracked(see col. 6, lines 46-67, col. 7, lines 3-19, 32-42).

16. As per claim 28, Copeland III discloses wherein the tracking database includes a comparison module for comparing the neural network assessment and associated information against a second assessment based upon a second network intrusion(0103-0104).

17. As per claim 29, Copeland III discloses tracking action is executed based upon an output from the comparison module(see 0103-0104, 0060-0061).

18. As per claims 12, 17, Copeland III discloses a traffic sorter that receives a copy of the network activity and sorts such all activities by IP/user for the purpose collecting continuous and sequential samples of each IP/user's activities/behaviors by IP/users wherein many packets are accumulated in any one sampling interval for each IP/user(0018, 0037, 0060-0061, 0165); an activity monitor operatively coupled to the traffic sorter for sequentially monitoring converted human intent behaviors and activities by IP/users(0018); an inter-port fusion module that fuses assessments from one or more assessment engines that monitor activities measures by port and non-port specific conversions(0051-0055); and an outcome director operatively coupled to the inter-port fusion monitor(0062-0067). Copeland discloses wherein the activity monitor(see 0018), wherein the at least one dedicated monitor includes an activity analysis module, behavior module, an activity translator module and an assessment module(0050-0065).

Copeland III does not disclose a trained back propagation network.

19. Botros et al. discloses a trained back propagation network(see col. 12, lines 25-51). It would have been obvious to include a back propagation of Botros with Copeland III, the motivation is that the motivation is that most attempted security violations are internal; that is, they are attempted by employees of an enterprise or organization(see col. 1, lines 48-52). Botros discloses detecting computer network intrusions is calculated based upon factors such as command sequences, user activity, machine usage loads, resource violations, files accessed, data transferred, terminal activity and network activity. These factors or input to a model or expert system, which determines whether a possible violation has occurred(see col. 1, lines 53-63). Thus, this is a method detects misuse of users within a network. It would have been obvious to include the back propagation network of Botros et al. with Copeland III, the motivation is that by including the back propagation network of Botros with Copeland III, is that the back propagation network includes a training algorithm that is used in network intrusion detection, to distinguish between normal behavior and anomalous behavior(see col. 12, lines 25-51 of Botros).

20. As per claim 18, Copeland III discloses wherein the activity monitor monitors the port specific activity information(0051-0055).

21. See motivation as per claim 1. As per claim 19, Botros et al. discloses wherein the activity translator module assigns a binary rating based upon presence(1) or absence(0) of at least one activity/behavior detected by the packet level analysis module(see col. 8, lines 40-67).

22. As per claim 20, Botros et al. discloses wherein the assessment module generates an assessment of levels of expertise and deception present in any sample of an IP/User's overall activities/behaviors for a collection interval(see col. 6, lines 53-65, col. 8, lines 46-67). The

motivation is that by giving an assessment of high or low, anomalous or normal behavior can be scored accordingly (see col. 13, lines 24-41 of Botros).

23. As per claim 22, Copeland III discloses wherein an outcome director initiates a tracking command based upon the assessment result(see 0062-0067).

24. As per claim 32, Copeland III discloses wherein the step of receiving includes creating a copy of the network activity sorted by users(see 0018, 0037, 0060-0061, 0165).

25. As per claim 33, Copeland III discloses the step of sorting non-port specific activity information from the received packet level activity information by the IP/user; and converting the non-port specific activity information to human behavioral measures of intent(see 0139, 0157-0158, 0197).

Response to Amendment

26. The Applicant states that the Applicant invention uses a back propagation network that provides a combined expertise and deception rating for each single monitored behavior. The Applicant states that the invention does not have a rule set, like in signature detection. Further, the Applicant states that a signature detection system cannot detect a new event if there is no predefined rule for that event. First, independent claims 1 and 31 do not claim, "detecting new events". Claims 1 and 31 disclose, "predefined behavior elements". Claim 12 discloses, "whether or not such combinations of behaviors and activities have been previously encountered". If the Applicant wishes to claim using a back propagation network for new behaviors or events, than the Applicant should claim in all independent claims.

27. The Applicant states that Lyle nor Botros disclose real-time assessment... processing in real-time the presence or absence of identified behavior elements... All remarks on page 12 by

Applicant fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

28. With regards to claim 12, Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

29. With regards to claim 31, Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

30. The Examiner has applied new art in place of Lyle with Copeland III. Copeland III more specifically discloses port scanning across network.

31. Claims 1 and 31 Applicant discloses, "non-signature and non-anomaly based". The Examiner was unable to find in the specification this distinction. In order to further prosecution, the Applicant is urged to change this to a binary representation. Also, in order to further prosecution, if the Applicant can amend the claims to more specifically, claim "an input vector representative of behavior is processed by the BPN with its output designated as behavioral ratings across expertise and deception domains. Combinations of monitored activity across the BPN and these includes those activities that have not been previously encountered. BPN rating consists of four cells, high deception/high expertise, HD/LE, LD/HE, LD/LE. The grid provides a view of assessed behavior. If the output assessed is a HD/HE than blocking action will occur.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

December 21, 2007

SYED A. ZIA
PRIMARY EXAMINER